

Efficient Codes for Adversarial Wiretap Channels

Pengwei Wang and Reihaneh Safavi-Naini

Department of Computer Science, University of Calgary, Canada

e-mail: [pengwwan, rei]@ucalgary.ca

Abstract—In [13] we proposed a (ρ_r, ρ_w) -adversarial wiretap channel model (AWTP) in which the adversary can adaptively choose to see a fraction ρ_r of the codeword sent over the channel, and modify a fraction ρ_w of the codeword by adding arbitrary noise values to them. In this paper we give the first efficient construction of a capacity achieving code family that provides perfect secrecy for this channel.

I. INTRODUCTION

In Wyner's wiretap model [15] channel noise in the channel is used as a resource for the system designer to provide (asymptotic) perfect secrecy against a computationally unbounded adversary without the need for a shared key. In this model, a sender and a receiver communicate over a noisy channel referred as the main channel, and their communication is eavesdropped by an adversary through a second noisy channel, referred to as the adversary channel. The goal is to provide (asymptotic) perfect reliable communication from sender to receiver with (asymptotic) perfect secrecy against the adversary. In this model adversary is passive and obstruction of its view by noise is probabilistic.

Recently a number of models [1], [4], [11] that include a stronger adversary that can modify communication have been introduced. These models primarily use arbitrarily varying channel approach and assume eavesdropper and jammer (who modifies communication) do not communicate. We introduced [13] an adversarial model for wiretap channel in which the adversary can adaptively choose a fraction of the communicated codeword to see and a fraction to modify. The modification of each component is by adding (algebraic) an arbitrary value (adversary's choice) to the component. The adversary's choice of observation and tampering components is unrestricted, as long as the total number of observation and tampering symbols are within specific limits. An Adversary Wiretap Channel (AWTP) is specific by two parameters (ρ_r, ρ_w) and is denoted by (ρ_r, ρ_w) -AWTP channel. An (ϵ, δ) -AWTP code guarantees that the information leaked about the message (measured using statistical distance) and the probability of decoding failure are upper bounded by ϵ and δ , respectively. The information rate of a code C is $R(C) = \frac{\log |\mathcal{M}|}{N \log |\Sigma|}$ where N is the length of the code and \mathcal{M} is the message space. The code provides perfect secrecy if $\epsilon = 0$.

We derived an upper bound on the rate of codes for (ρ_r, ρ_w) -AWTP channels as $R(C) \leq 1 - \rho_r - \rho_w + 2\epsilon \log_{|\Sigma|} \frac{1}{\epsilon}$, and code family with perfect secrecy is $R(C) \leq 1 - \rho_r - \rho_w$. An explicit and inefficient construction of AWTP code is also given in [13].

A. Our Result

We give an efficient construction of a code family $\mathcal{C} = \{C^N; N \in \mathbb{Z}\}$ in which every code C^N of length N , provides perfect secrecy for a (ρ_r, ρ_w) -AWTP channel. The construction uses three building blocks: an Algebraic Manipulate Detection Code (AMD code) [5], a Subspace Evasive Sets. (SES) [7], and a Folded Reed-Solomon code (FRS code) [8]. AMD code detects algebraic manipulation assuming the adversary is oblivious and does not have access to the codeword. SES are subsets with the property that their intersection with any subset of certain dimension is bounded. FRS code is a special class of Reed-Solomon code that achieve list decoding capacity, and have efficient encoding and decoding. Encoding of a message uses the three building blocks in order: the message is encoded using AMD code, then using a SES and finally an FRS code. In decoding, first the FRS decoder outputs a list of possible codewords. This list for the decoding algorithm in [8], is a function of N , the code length. Using the intersection algorithm of SES the list can be pruned to a shorter list which is independent of the code length. The final step is to use the AMD code to find the correct message. The decoder always outputs the correct message. We prove with appropriate choice of parameters, each code in the family is perfectly secure, satisfies the upper bound on rate for (ρ_r, ρ_w) -AWTP channels with equality and so is capacity achieving, and finally the probability of decoding error reduces exponentially in N .

B. Related Work

Wiretap channels have been an active area of research for a number of years with excellent progress on extending the model and strengthening security against passive adversary [2], [3], [6], [9]–[12]. More recently active adversary for these channels have been considered [1], [4], [11], [13]. The active adversary in [4], [11] is modeled using arbitrarily varying channels, and is assumed that there is no communication between the eavesdropper and the wiretapper. In [1] the wiretap II model is extended to active adversary. The adversary however is restricted to flip the codeword components that they have chosen to read. In [14] we proposed a model for adversarial channel called *limited view adversarial channel* (LVAC), which is the same as the adversarial channel considered here. The goal of communication however was reliability only. (ρ_r, ρ_w) -AWTP channels have the same adversary power as LVAC channel, but the goal of communication is reliability and privacy both.

Paper organization: In section II, we recall the model and capacity results for (ρ_r, ρ_w) -AWTP channels. In section III,

we give our construction and conclude the paper in section IV.

II. MODEL AND DEFINITIONS

We consider the following scenario. Alice (Sender \mathcal{S}) wants to send messages $m \in \mathcal{M}$ securely and reliably to Bob (Receiver \mathcal{R}), over a communication channel that is partially controlled by Eve (Adversary). Let $[N] = \{1, \dots, N\}$. $S_r = \{i_1, \dots, i_{\rho_r N}\} \subseteq [N]$ and $S_w = \{j_1, \dots, j_{\rho_w N}\} \subseteq [N]$ denote two subsets of the N coordinates. For a vector x , $\text{SUPP}(x)$ denotes the set of coordinates where x_i is non-zero. Let Σ denote the code alphabet, with an underlying group operation.

Definition 1: [13] A (ρ_r, ρ_w) -Adversarial Wiretap channel $((\rho_r, \rho_w)$ -AWTP channel), is an adversarially corrupted communication channel between Alice and Bob such that it is (partially) controlled by an adversary Eve, with two capabilities: Reading and Writing. In *Reading* (or *Eavesdropping*), Eve selects a subset $S_r \subseteq [N]$ of size at most $\rho_r N$ and sees the components of the sent codeword c on S_r . Eve's view of the codeword is the set of all read components: $\text{View}_{\mathcal{A}}(\text{AWTPenc}(m, r_S), r_{\mathcal{A}}) = \{c_{i_1}, \dots, c_{i_{\rho_r N}}\}$. In *Writing* (or *Jamming*), Eve chooses a subset $S_w \subseteq [N]$ of size at most $\rho_w N$ and adds an error vector e to c , where the addition is component-wise and over Σ . We require $\text{SUPP}(e) = S_w$. The corrupted components of c are $\{y_{j_1}, \dots, y_{j_{\rho_w N}}\}$ and $y_{j_\ell} = c_{j_\ell} + e_{j_\ell}$. The error e is generated according to the Eve's best strategy to make Bob's decoder fail.

The adversary is *adaptive* and selects components of c for reading and writing, one by one and at each step using its knowledge of the codeword at that time.

Alice and Bob will use an *Adversarial Wiretap Code* to provide security and reliability for communication over Adversary wiretap channel.

Definition 2: [13] An $(\mathcal{M}, N, \Sigma, \epsilon, \delta)$ -AWTP Code $((\epsilon, \delta)$ -AWTP code for short) for a (ρ_r, ρ_w) -AWTP channel consists of a randomized encoding $\text{AWTPenc} : \mathcal{M} \times \mathcal{U} \rightarrow \mathcal{C}$, from the message space \mathcal{M} to a code \mathcal{C} , and a deterministic decoding algorithm $\text{AWTPdec} : \Sigma^N \rightarrow \{\mathcal{M} \cup \perp\}$, such that $\text{AWTPdec}(\text{AWTPenc}(m, r_S)) = m$ for all $m \in \mathcal{M}$. The code guarantees secrecy and reliability as defined below.

i) *Secrecy:* For any two messages $m_1, m_2 \in \mathcal{M}$, we have

$$\text{Adv}^{\text{ds}}(\text{AWTPenc}, \text{View}_{\mathcal{A}}) \triangleq \max_{m_0, m_1} \text{SD}(\text{View}_{\mathcal{A}}(\text{AWTPenc}(m_1), r_{\mathcal{A}}), \text{View}_{\mathcal{A}}(\text{AWTPenc}(m_2), r_{\mathcal{A}})) \leq \epsilon$$

Here we assume the adversary uses the same random coins $r_{\mathcal{A}}$ for the encoding of two messages.

ii) *Reliability:* For any message m that is encoded to c by the sender, and corrupted to $y = c + e$ by the (ρ_r, ρ_w) -AWTP channel, the probability that the receiver outputs the correct information m is at least $1 - \delta$. Receiver will output \perp with probability no more than δ and will never output an incorrect message. That is,

$$\mathbb{P}[\text{AWTPdec}(\text{AWTPenc}(m) + e) = \perp] \leq \delta$$

An AWTP code is *perfectly secure* if $\epsilon = 0$.

Definition 3: For a fixed $\epsilon > 0$, an ϵ -secure AWTP code family is a family $\mathbb{C} = \{C^N\}_{N \in \mathbb{N}}$ of (ϵ, δ_N) -AWTP codes indexed by $N \in \mathbb{N}$, for a (ρ_r, ρ_w) -AWTP channel. When $\epsilon = 0$, the family is called a *perfectly secure AWTP code family*.

Definition 4: For a family \mathbb{C} of (ϵ, δ) -AWTP codes the *rate* $R(\mathbb{C})$ is *achievable* if for any $\xi > 0$, there exists N_0 such that for any $N \geq N_0$, we have, $\frac{1}{N} \log_{|\Sigma|} |\mathcal{M}_N| \geq R(\mathbb{C}) - \xi$, and the probability of decoding error is $\delta \leq \xi$.

We use the achievable rate of a code family for an AWTP channel to define secrecy capacity of the channel.

Definition 5: The ϵ -secrecy (perfect secrecy) capacity of a (ρ_r, ρ_w) -AWTP channel denoted by \mathbf{C}^ϵ (\mathbf{C}^0), is the largest achievable rate of all (ϵ, δ) -AWTP $((0, \delta)$ -AWTP) code families \mathbb{C} for the channel.

The following upper bounds are derived in [13].

Lemma 1: [13] The ϵ -secrecy capacity of a (ρ_r, ρ_w) -AWTP channel satisfies the upper bound,

$$\mathbf{C}^\epsilon \leq 1 - \rho_r - \rho_w + 2\epsilon \rho_r N \log_{|\Sigma|} (1 + \frac{1}{\epsilon})$$

The upper bound for the perfect secrecy capacity of a (ρ_r, ρ_w) -AWTP channel is, $\mathbf{C}^0 \leq 1 - \rho_r - \rho_w$.

III. AN EFFICIENT CAPACITY ACHIEVING AWTP-CODE

The general approach to the construction was outlined in Section I-A. Below we recall the definition of the building blocks, and give our instantiations, and construction of the code.

1) *Algebraic Manipulation Detection Code (AMD code):*

Consider a storage device $\Sigma(\mathcal{G})$ that holds an element x from a group \mathcal{G} . The storage $\Sigma(\mathcal{G})$ is private but can be manipulated by the adversary by adding $\Delta \in \mathcal{G}$. AMD code allows the manipulation to be detected.

Definition 6 (AMD-code [5]): An $(\mathcal{X}, \mathcal{G}, \delta)$ -Algebraic Manipulation Detection code $((\mathcal{X}, \mathcal{G}, \delta)$ -AMD code) consists of two algorithms (AMDenc, AMDdec). Encoding given by, AMDenc : $\mathcal{X} \rightarrow \mathcal{G}$, is probabilistic and maps an element of a set \mathcal{X} to an element of an additive group \mathcal{G} . Decoding, AMDdec : $\mathcal{G} \rightarrow \mathcal{X} \cup \{\perp\}$, is deterministic and we have AMDdec(AMDenc(x)) = x , for any $x \in \mathcal{X}$. Security of AMD codes is defined by requiring,

$$\mathbb{P}[\text{AMDdec}(\text{AMDenc}(x) + \Delta) \in \{x, \perp\}] \leq \delta, \quad (1)$$

for all $x \in \mathcal{X}, \Delta \in \mathcal{G}$.

An AMD code is *systematic* if the encoding has the form AMDenc : $\mathcal{X} \rightarrow \mathcal{X} \times \mathcal{G}_1 \times \mathcal{G}_2$, $x \rightarrow (x, r, t = f(x, r))$ for some function f and $r \xleftarrow{\$} \mathcal{G}_1$. The decoding function AMDdec(x, r, t) = x if and only if $t = f(x, r)$ and \perp otherwise.

We use a systematic AMD-code that is based on the extension of the construction in [5] to extension fields. Let ϕ be a bijection between vectors \mathbf{v} of length N over \mathbb{F}_q , and elements in \mathbb{F}_{q^N} , and let ℓ be an integer such that $\ell + 2$ is not divisible

by q . Define the function $\text{AMDenc} : \mathbb{F}_{q^N}^\ell \rightarrow \mathbb{F}_{q^N}^\ell \times \mathbb{F}_{q^N} \times \mathbb{F}_{q^N}$ by $\text{AMDenc}(x) = (x, r, f(x, r))$ where

$$f(x, r) = \phi^{-1} \left(\phi(r)^{\ell+2} + \sum_{i=1}^{\ell} \phi(x_i) \phi(r)^i \right) \mod q^N$$

Lemma 2: For the AMD-code above, given a codeword (x, r, t) , the success chance of an adversary that has no information about (x, r, t) , in constructing a new codeword $(x', r', t') = (x' = x + \Delta x, r' = r + \Delta r, t' = t + \Delta t)$, that passes the verification $t' = f(x', r')$ is at most $\frac{\ell+1}{q^N}$.

2) *Subspace Evasive Sets:* We briefly introduce subspace evasive sets. More details can be found in Appendix A.

Definition 7 (Subspace Evasive Sets [7], [8]): Let $\mathcal{S} \subset \mathbb{F}_q^n$. We say \mathcal{S} is (v, ℓ_{SE}) -subspace evasive if for all v -dimensional affine subspaces $\mathcal{H} \subset \mathbb{F}_q^n$, we have $|\mathcal{S} \cap \mathcal{H}| \leq \ell_{\text{SE}}$.

Dvir *et al.* [7] show that there is an efficient construction for subspace evasive sets $\mathcal{S} \subset \mathbb{F}_q^n$, and an efficient *intersection algorithm* to compute $\mathcal{S} \cap \mathcal{H}$ for any v -dimensional subspace $\mathcal{H} \subset \mathbb{F}_q^n$.

Lemma 3: [7] Let $v, n_1 \in \mathbb{N}$, $w = v^2$, $n = \frac{n_1}{w-v}w$ and \mathbb{F}_q be a finite field. Then there is a $(v, v^{v \cdot C \log \log v})$ -subspace evasive set $\mathcal{S} \subset \mathbb{F}_q^n$. For any vector $\mathbf{v} \in \mathbb{F}_q^{n_1}$, there is a bijection which maps \mathbf{v} into an elements of the subspace evasive set. That is

$$\text{SE} : \mathbf{v} \rightarrow \mathbf{v}' \in \mathcal{S}$$

Lemma 4: [7] Let $\mathcal{S} \subset \mathbb{F}_q^n$ be the (v, ℓ_{SE}) -subspace evasive set. There exists an algorithm that, given a basis for any \mathcal{H} , output $\mathcal{S} \cap \mathcal{H}$ in $\mathcal{O}(v^{v \cdot \log \log v})$ time.

3) *Folded Reed-Solomon Code (FRS code):* A error correcting code C is a subspace of \mathbb{F}_q^N . The rate of the code is $\log_2 |C|/N$. A code C of length N and rate R is $(\rho, \ell_{\text{List}})$ -list decodable if the number of codewords within distance ρN from any received word is at most ℓ_{List} . List decodable codes can potentially correct up to $1 - R$ fraction of errors, which is twice that of unique decoding. This is however at the cost of outputting a list of possible sent codewords (messages). Construction of good code with efficient list decoding algorithms is an important research question. An explicit construction of a list decodable code that achieves the list decoding capacity $\rho = 1 - R - \varepsilon$ is given by Guruswami *et al.* [8]. The code is called *Folded Reed-Solomon codes (FRS codes)*, defined by Guruswami *et al.* [8], gives an explicit construction for list decodable codes that achieve the list decoding capacity $\rho = 1 - R - \varepsilon$. The code has polynomial time encoding and decoding algorithms.

Definition 8: [8] A u -Folded Reed-Solomon code is an error correcting code with block length N over \mathbb{F}_q^u and $q > Nu$. The message of an FRS code is written in the form of a polynomial $f(x)$ with degree k over \mathbb{F}_q . The FRS codeword corresponding to the message is a vector over \mathbb{F}_q^u where each component is a u -tuple $(f(\gamma^{ju}), f(\gamma^{ju+1}), \dots, f(\gamma^{ju+u-1}))$, $0 \leq j < N$, where γ is a generator of \mathbb{F}_q^* , the multiplicative group of \mathbb{F}_q . A codeword of a u -folded Reed-Solomon code of length N is in one-to-one correspondence with a codeword

c of a Reed-Solomon code of length uN , and is obtained by grouping together u consecutive components of c . We use FRSenc to denote the encoding algorithm of the FRS code. u is called the *folding parameter* of the FRS code.

We will use the *linear algebraic FRS decoding algorithm* of these codes [8] (Appendix B-A). The following Lemma gives the decoding capability of linear algebraic FRS code.

Lemma 5: [8] For a Folded Reed-Solomon code of block length N and rate $R = \frac{k}{uN}$, the following holds for all integers $1 \leq v \leq u$. Given a received word $y \in (\mathbb{F}_q^u)^N$ agreeing with c in at least a fraction,

$$N - \rho N > N \left(\frac{1}{v+1} + \frac{v}{v+1} \frac{uR}{u-v+1} \right)$$

one can compute a matrix $\mathbf{M} \in \mathbb{F}_q^{k \times (v-1)}$ and a vector $\mathbf{z} \in \mathbb{F}_q^k$ such that the message polynomials $f \in \mathbb{F}_q[X]$ in the decoded list are contained in the affine space $\mathbf{M}\mathbf{b} + \mathbf{z}$ for $\mathbf{b} \in \mathbb{F}_q^{v-1}$ in $\mathcal{O}((Nu \log q)^2)$ time.

A. An Explicit Capacity Achieving $(0, \delta)$ -AWTP Code Family

Let \mathcal{M} denote the message space, N denote the code length and the encoding and decoding algorithms be, AWTPenc_N and AWTPdec_N , respectively. The message, also referred to as the information block of the AWTP code, is $\mathbf{m} = \{m_1, \dots, m_{uRN}\} \in \mathcal{M}$ where $m_i \in \mathbb{F}_q$. Let \mathcal{S} be a $(v, v^{C \cdot v \cdot \log \log v})$ -subspace evasive set in $\mathbb{F}_q^{n_1}$. Let u and v denote the folding and the interpolation parameters of the FRS code, respectively. Let q be a prime number larger than Nu , γ be a primitive element of \mathbb{F}_q , $\ell = \lceil uR \rceil$, $w = v^2$, $b = \lceil \frac{\ell N + 2N}{w-v} \rceil$, $n_1 = (w-v)b$, $n = wb$, $\text{SE} : \mathbb{F}_q^{n_1} \rightarrow \mathcal{S}$ be the bijection of subspace evasive set.

The construction of encoder and decoder for C^N is given in Figure III-A.

Figure III-A

Encoding: For a code rate R , the sender \mathcal{S} does the following.

- 1) Start with the information block \mathbf{m} of length uRN . Append sufficient zeros $N(\ell - uR)$ to construct a vector \mathbf{x} of length $N\ell$; that is, $\mathbf{x} = \{\mathbf{m} || 0, \dots, 0\}$.
- 2) Generate a random vector \mathbf{r} with length N over \mathbb{F}_q . Use the AMD construction in section III-1 to construct the AMD codeword $\{\mathbf{x}, \mathbf{r}, \mathbf{t}\}$. That is, $\text{AMDenc}(\mathbf{x}) = \{\mathbf{x}, \mathbf{r}, \mathbf{t}\}$. The length of AMD code is $\ell N + 2N$.
- 3) Extend the AMD codeword to length n_1 by appending zeros. Encode AMD code into an element \mathbf{s} of the subspace evasive set \mathcal{S} . The length of \mathbf{s} is n . That is

$$\mathbf{s} = \text{SE}(\mathbf{x}, \mathbf{r}, \mathbf{t} || 0, \dots, 0)$$

- 4) Append a random vector $\mathbf{a} = \{a_1 \dots a_{u\rho_r N}\} \in \mathbb{F}_q^{u\rho_r N}$ to \mathbf{s} to form a vector that will be the message of the FRS code, and interpret that as

coefficients of the polynomial $f(x)$ over \mathbb{F}_q . That is $\{f_0, \dots, f_{k-1}\} = (\mathbf{s} || \mathbf{a})$. We have $k = \deg(f) + 1 = u\rho_r N + n$.

- 5) Use FRSenc to construct the FRS codeword $c = \text{FRSenc}(f(X)) = \{c_1, \dots, c_N\}$, and $c_i = \{f(\gamma^{i(u-1)}), \dots, f(\gamma^{iu-1})\} \in \mathbb{F}_q^u$, $i = 1, \dots, N$.

Decoding: The receiver \mathcal{R} does the following:

- 1) Let $y = c + e$, and $w_H(e) \leq \rho_w N$. The i -th component of y is $y_i = \{y_{i,1}, \dots, y_{i,u}\}$ for $i = 1, \dots, N$.
- 2) Use the FRS decoding algorithm $\text{FRSdec}(y)$ to output a matrix $\mathbf{M} \in \mathbb{F}_q^{k \times v}$ and a vector $\mathbf{z} \in \mathbb{F}_q^k$, such that the codewords in the output list are, $\mathcal{L}_{\text{FRS}} = \mathbf{M}\mathbf{b} + \mathbf{z}$. \mathbf{M} has k rows each giving a component of the output vector as a linear combination of $\{b_1, \dots, b_v\}$. Let \mathcal{H} denote the space which is generated by the first n equations. That is

$$\mathcal{H} = \mathbf{M}_{n \times v} \mathbf{b} + \mathbf{z}_n, \mathbf{b} \in \mathbb{F}_q^v,$$

where $\mathbf{M}_{n \times v}$ is the first n rows of the submatrix of $\mathbf{M}_{n \times v}$ and \mathbf{z}_n is the first n elements of \mathbf{z} .

- 3) The decoder calculates the intersection $\mathcal{S} \cap \mathcal{H}$ and outputs a list \mathcal{L} with size at most $v^{C \cdot v \cdot \log \log v}$. Each $\mathbf{s}_i \in \mathcal{L}$ corresponds to an AMD codeword $\{\mathbf{x}_i, \mathbf{r}_i, \mathbf{t}_i\}$.
- 4) For each AMD codeword $\{\mathbf{x}_i, \mathbf{r}_i, \mathbf{t}_i\}$, the decoder verifies $\mathbf{t}_i = f(\mathbf{x}_i, \mathbf{r}_i)$. If there is a unique valid AMD codeword, the decoder outputs the first uRN components of \mathbf{x} as the correct message \mathbf{m} . Otherwise, outputs \perp .

We prove secrecy and reliability, and derive the rate of AWTP code family.

Lemma 6 (Secrecy): The AWTP code C provides perfect security for (ρ_r, ρ_w) -AWTP channel.

Proof: We show that an AWTP codeword sent over an (ρ_r, ρ_w) -AWTP channel leak no information about the encoded subspace evasive sets element \mathbf{s} and so the message \mathbf{m} will remain perfectly secure. Let $S, A, C^{[r]}$ denote the random variables corresponding to \mathbf{s}, \mathbf{a} and $c^{[r]} = \{c_{j1}, \dots, c_{j\rho_r N}\}$, respectively. For an adversary observation $\{c_{i1}, \dots, c_{i\rho_r N}\}$ with $c_{ij} = \{c_{ij,1}, \dots, c_{ij,u}\} \in \mathbb{F}_q^u$, using the FRS encoding equations, the adversary has the following $u\rho_r N$ equations.

$$\begin{bmatrix} 1 & \gamma^{(i_1-1)u} & \dots & \gamma^{(i_1-1)u(k-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \gamma^{i_1 u-1} & \dots & \gamma^{(i_1 u-1)(k-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \gamma^{(i_{\rho_r N}-1)u} & \dots & \gamma^{(i_{\rho_r N}-1)u(k-1)} \\ \vdots & \vdots & \dots & \vdots \\ 1 & \gamma^{i_{\rho_r N} u-1} & \dots & \gamma^{(i_{\rho_r N} u-1)(k-1)} \end{bmatrix} \times \begin{bmatrix} \mathbf{s} \\ \mathbf{a} \end{bmatrix} = \begin{bmatrix} c_{i_1,1} \\ \vdots \\ c_{i_1,u} \\ \vdots \\ c_{i_{\rho_r N},1} \\ \vdots \\ c_{i_{\rho_r N},u} \end{bmatrix}$$

It is easy to see that \mathbf{s} together with the randomness \mathbf{a} uniquely determines $\mathbf{c}^{[r]}$. This gives,

$$\mathbb{P}(C^{[r]} = \mathbf{c}^{[r]} | \{S, A\} = \{\mathbf{s}, \mathbf{a}\}) = 1. \quad (2)$$

Conversely, for given values of \mathbf{s} and $\{c_{i1}, \dots, c_{i_{\rho_r N}}\}$, and noting that the coefficient matrix is Vandermonde, there exists a unique solution for the $u\rho_r N$ unknown components of $\mathbf{a} = \{a_1, \dots, a_{u\rho_r N}\} \in \mathbb{F}_q^{u\rho_r N}$. That is

$$\mathbb{P}(A = \mathbf{a} | \{S, C^{[r]}\} = \{\mathbf{s}, \mathbf{c}^{[r]}\}) = 1 \quad (3)$$

Since \mathbf{a} is chosen uniformly and independent of \mathbf{s} , we have

$$\mathbb{P}(A = \mathbf{a} | S = \mathbf{s}) = \frac{1}{q^{u\rho_r N}} \quad (4)$$

From (2),(3), and (4) we have,

$$\begin{aligned} \mathbb{P}(C^{[r]} = \mathbf{c}^{[r]}, A = \mathbf{a} | S = \mathbf{s}) \\ = \mathbb{P}(A = \mathbf{a} | \{S, C^{[r]}\} = \{\mathbf{s}, \mathbf{c}^{[r]}\}) \mathbb{P}(C^{[r]} = \mathbf{c}^{[r]} | S = \mathbf{s}) \\ = \mathbb{P}(C^{[r]} = \mathbf{c}^{[r]} | \{S, A\} = \{\mathbf{s}, \mathbf{a}\}) \mathbb{P}(A = \mathbf{a} | S = \mathbf{s}), \end{aligned}$$

which implies for any \mathbf{s} ,

$$\mathbb{P}(C^{[r]} = \mathbf{c}^{[r]} | S = \mathbf{s}) = \frac{1}{q^{u\rho_r N}}. \quad (5)$$

This means that for any two elements \mathbf{s}_1 and \mathbf{s}_2 of the subspace evasive sets,

$$\begin{aligned} \text{SD}(\text{View}_A | \mathbf{s}_1, \text{View}_A | \mathbf{s}_2) \\ = \sum_{\mathbf{c}^{[r]} \in \text{View}_A} \frac{1}{2} |\mathbb{P}(\mathbf{c}^{[r]} | \mathbf{s}_1) - \mathbb{P}(\mathbf{c}^{[r]} | \mathbf{s}_2)| = 0 \end{aligned}$$

Lemma 7 (Reliability): The failure probability of AWTPdec_N is bounded by $\delta_N \leq \frac{v^{C \cdot v \cdot \log \log v}}{q^N}$. ■

Proof: The FRS decoder outputs a list of elements of the subspace evasive $\mathbf{s}_i \in \mathcal{L}$ with list size at most $\ell_{\text{SE}} \leq v^{C \cdot v \cdot \log \log v}$. Each element corresponds to a unique AMD codeword $\{\mathbf{x}_i, \mathbf{r}_i, \mathbf{t}_i\} = \text{SE}^{-1}(\mathbf{s}_i)$.

We first show that the correct message \mathbf{m} will be always output by the receiver. Denote the AMD codeword corresponding to the message \mathbf{m} as $\{\mathbf{x}, \mathbf{r}, \mathbf{t}\} = \text{AMDenc}(\mathbf{m} || 0, \dots, 0)$. The list decoding algorithm outputs codewords that are at distance at most $\rho_w N$ of the received word and so include the original codeword. The bijection function SE, encodes the AMD codeword into an element of the subspace evasive set $\mathbf{s} \in \mathcal{S}$ that belongs to the decoded list $\mathbf{s} \in \mathcal{H}$ that passes AMD verification. That is,

$$\text{SE}(\mathbf{x}, \mathbf{r}, \mathbf{t} || 0, \dots, 0) \in \mathcal{L} = \mathcal{S} \cap \mathcal{H} \text{ and } \mathbf{t} = f(\mathbf{x}, \mathbf{r})$$

Second, we show that the probability that any other codeword in the list is a valid AMD codeword is small. That is we will show that,

$$\mathbb{P}(\{\mathbf{x}', \mathbf{r}', \mathbf{t}'\} = \text{SE}^{-1}(\mathbf{s}') \wedge \mathbf{s}' \in \mathcal{L} \wedge \mathbf{t}' = f(\mathbf{x}', \mathbf{r}')) \leq \frac{\ell}{q^N}$$

From Lemma 6, the adversary has no information about the encoded subspace evasive sets element \mathbf{s} and the AMD

codeword $\{\mathbf{x}, \mathbf{r}, \mathbf{t}\} = \text{SE}^{-1}(\mathbf{s})$ and so the adversary error, $\{\Delta \mathbf{x}_i = \mathbf{x}' - \mathbf{x}, \Delta \mathbf{r}_i = \mathbf{r}' - \mathbf{r}, \Delta \mathbf{t}_i = \mathbf{t}' - \mathbf{t}\}$, is independent of $\{\mathbf{x}, \mathbf{r}, \mathbf{t}\}$. According to Lemma 2, the probability that the tampered AMD codeword, $\{\mathbf{x}', \mathbf{r}', \mathbf{t}'\}$, passes the verification is no more than $\frac{\ell}{q^N}$.

Finally, we show the unique correct message output by receiver with probability at least $1 - \frac{v^{C' \cdot v \cdot \log \log v}}{q^N}$. The list size is at most $v^{C \cdot v \cdot \log \log v}$ and $\ell \leq u = v^2$. So the probability that any $\{\mathbf{x}', \mathbf{r}', \mathbf{t}'\} \neq \{\mathbf{x}, \mathbf{r}, \mathbf{t}\}$ in decoding list pass the verification $\mathbf{t}' = f(\mathbf{x}', \mathbf{r}')$, is no more than $\frac{v^{(C+2) \cdot v \cdot \log \log v}}{q^N}$. That is

$$\begin{aligned} & \mathbb{P}\left(\bigcup_{\mathbf{s}' \in \mathcal{L}} \{\mathbf{x}', \mathbf{r}', \mathbf{t}'\} = \text{SE}^{-1}(\mathbf{s}') \wedge \mathbf{t}' = f(\mathbf{x}', \mathbf{r}')\right) \\ & \leq \sum_{\mathbf{s}' \in \mathcal{L}} \mathbb{P}(\{\mathbf{x}', \mathbf{r}', \mathbf{t}'\} = \text{SE}^{-1}(\mathbf{s}') \wedge \mathbf{t}' = f(\mathbf{x}', \mathbf{r}')) \\ & \leq \sum_{\mathbf{s}' \in \mathcal{L}} \mathbb{P}(\mathbf{t}' = f(\mathbf{x}', \mathbf{r}')) \leq \frac{\ell |\mathcal{L}|}{q^N} \leq \frac{v^{(C+2) \cdot v \cdot \log \log v}}{q^N} \end{aligned}$$

We first find the information rate of the code C^N , and then find the achievable rate of the code family \mathbb{C} .

Lemma 8 (Rate of C^N): The AWTP code C^N described above provides reliability for a (ρ_r, ρ_w) -AWTP channel if the following holds:

$$\rho_w < \frac{v}{v+1} - \frac{v}{v+1} \frac{\frac{v}{v-1}(uR+3) + u\rho_r}{u-v+1}. \quad (6)$$

Proof is in Appendix C.

Lemma 9 (Achievable Rate of \mathbb{C}): The information rate of the $(0, \delta)$ -AWTP code family $\mathbb{C} = \{C^N\}_{N \in \mathbb{N}}$ for a (ρ_r, ρ_w) -AWTP channel is $R(\mathbb{C}) = 1 - \rho_r - \rho_w$.

Proof: For a given small $\frac{1}{2} > \xi > 0$, let code parameters be chosen as, $\xi_1 = \frac{\xi}{13}$, $v = 1/\xi_1$ and $u = 1/\xi_1^2$. Finally let, $N_0 > (1/\xi)^{C/\xi \log \log 1/\xi}$ where $C > 0$ is constant. From

$$1 - R - \rho_r - 12\xi_1 \leq \frac{1}{\xi_1 + 1} - \frac{1}{\xi_1 + 1} \frac{\frac{1}{1-\xi_1}(R + 3\xi_1^2) + \rho_r}{1 - \xi_1 + \xi_1^2}$$

the decoding condition (6) of AWTP code is satisfied if,

$$\rho_w < 1 - R - \rho_r - 12\xi_1. \quad (7)$$

We choose $R = 1 - \rho_r - \rho_w - 12\xi_1$, the decoding condition of AWTP code will be satisfied. Now since $\xi = 13\xi_1$, for any $N > N_0$, the rate of the AWTP code C^N is

$$\begin{aligned} \frac{1}{N} \log_{|\Sigma|} |\mathcal{M}_N| &= R = 1 - \rho_r - \rho_w - 12\xi_1 \\ &> 1 - \rho_r - \rho_w - \xi = R(\mathbb{C}) - \xi \end{aligned}$$

and the probability of decoding error,

$$\delta_N \leq (1/\xi)^{C/\xi \log \log 1/\xi} q^{-N} \leq Nq^{-N} \leq \xi$$

So the information rate of AWTP code family \mathbb{C} is $R(\mathbb{C}) = 1 - \rho_r - \rho_w$.

The computational time for encoding is $\mathcal{O}((N \log q)^2)$. The decoding of FRS code and intersection algorithm of

the subspace evasive set is $\mathcal{O}((1/\xi)^{C/\xi \log \log 1/\xi})$. The AMD verification is $\mathcal{O}((1/\xi)^{C/\xi \log \log 1/\xi} (N \log q)^2)$. So the total computational time of decoding is $\mathcal{O}((N \log q)^2)$.

Theorem 1: For any small $\xi > 0$, there is $(0, \delta)$ -AWTP code C^N of length N over (ρ_r, ρ_w) -AWTP channel such that the information rate is $R(C^N) = 1 - \rho_r - \rho_w - \xi$, the size of alphabet is $|\Sigma| = \mathcal{O}(q^{1/\xi^2})$ and decoding error $\delta < q^{-\mathcal{O}(N)}$. The computational time is $\mathcal{O}((N \log q)^2)$. The AWTP code family $\mathbb{C} = \{C^N\}_{N \in \mathbb{N}}$ achieves secrecy capacity $R(\mathbb{C}) = 1 - \rho_r - \rho_w$ for (ρ_r, ρ_w) -AWTP channel.

IV. CONCLUDING REMARKS

$((\rho_r, \rho_w))$ -AWTP extends Wyner wiretap models [1] to include active corruption at physical layer of communication channel. Although corruption in our general model is additive, for $S_w \subset S_r$, it is equivalent to arbitrary replacement of code components. We proposed an efficient construction for a capacity achieving code family for (ρ_r, ρ_w) -AWTP channels. The alphabet size for the code is \mathbb{F}_q^u where for $\delta < \xi$, $u = \mathcal{O}(\frac{1}{\xi^2})$. That is for small failure probability, larger size alphabet must be used. Constructing capacity achieving codes over small (fixed) size alphabets remains an open problem.

ACKNOWLEDGMENT

This research is in part supported by Alberta Innovates Technology Future, in the province of Alberta, Canada.

REFERENCES

- [1] V. Aggarwal, L. Lai, A. Calderbank, and H. Poor, "Wiretap Channel Type II with an Active Eavesdropper", *ISIT*, pp. 1944–1948, 2009.
- [2] M. Bellare, S. Tessaro, and A. Vardy, "Semantic Security for the Wiretap Channel", *CRYPTO*, pp. 294–311, 2012.
- [3] M. Bloch, and J. Barros, "Physical-Layer Security: From Information Theory to Security Engineering", *Cambridge Academic Press*, 2011.
- [4] H. Boche, and R. Schaefer, "Capacity Results and Super-Activation for Wiretap Channels With Active Wiretappers", *IEEE Transactions on Information Forensics and Security*, vol. 8(9) pp. 1482–1496, 2013.
- [5] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs, "Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors", *EUROCRYPT*, pp. 471–488, 2008.
- [6] I. Csiszar and J. Körner, "Broadcast Channels with Confidential Messages", *IEEE Transaction on Information Theory*, vol. 24(3), pp. 339–348, 1978.
- [7] Z. Dvir, and S. Lovett, "Subspace evasive sets", *STOC*, pp. 351–358, 2012.
- [8] V. Guruswami, "Linear Algebraic List Decoding of Folded Reed-Solomon Codes", *IEEE Conference on Computational Complexity*, pp. 77–85, 2011.
- [9] Leung-Yan-Cheong, and E. Hellman, "The Gaussian wire-tap channel", *IEEE Transactions on Information Theory*, vol. 24(4), pp. 451 – 456, 1978.
- [10] H. MahdaviFar, and A. Vardy, "Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes", *IEEE Transactions on Information Theory*, vol. 57, pp. 6428–6443, 2011.
- [11] E. MolavianJazi, M. Bloch, and J. N. Laneman, "Arbitrary Jamming Can Preclude Secure Communication", *47th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1069–1075, 2009.
- [12] L. Ozarow, and A. Wyner, "Wire-Tap Channel II", *EUROCRYPT*, pp. 33–50, 1984.
- [13] P. Wang and R. Safavi-Naini, "A Model for Adversarial Wiretap Channel", *CoRR abs/1312.6457*(2013).
- [14] R. Safavi-Naini, and P. Wang, "Codes for Limited View Adversarial Channels", *ISIT*, pp. 266–270, 2013.
- [15] A. Wyner, "The wire-tap channel", *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

APPENDIX A SUBSPACE EVASIVE SETS

Recently, Guruswami et al. [8] showed that the subspace evasive sets can be used to reduce the list size of list decoding algorithm. Dvir et al. [7] gives a explicit and efficient construction of subspace evasive sets. We briefly introduce Dvir et al. [7]'s construction of subspace evasive sets. In detail, we give the definition of subspace evasive set, the construction, the encoding function, and the bound of the size of intersection between subspace evasive sets and any v -dimensional space.

Definition 9: [8] [7] Let $\mathcal{S} \subset \mathbb{F}^n$. We say \mathcal{S} is (v, ℓ_{SE}) -subspace evasive sets if for all v -dimensional affine subspaces $\mathcal{H} \subset \mathbb{F}^n$, there is $|\mathcal{S} \cap \mathcal{H}| \leq \ell_{SE}$.

A. Construction of Subspace Evasive Set

Let \mathbb{F} be a field and $\overline{\mathbb{F}}$ be its algebraic closure. A variety in $\overline{\mathbb{F}}^w$ is the set of common zeros of one or more polynomials. Given v polynomials $f_1, \dots, f_v \in \overline{\mathbb{F}}[x_1, \dots, x_w]$, we denote the variety as

$$\mathbf{V}(f_1, \dots, f_v) = \{\mathbf{x} \in \overline{\mathbb{F}}^w \mid f_1(\mathbf{x}) = \dots = f_v(\mathbf{x}) = 0\}$$

where $\mathbf{x} = \{x_1, \dots, x_w\}$.

For a polynomials $f_1, \dots, f_v \in \mathbb{F}[x_1, \dots, x_w]$, we define the common solutions in \mathbb{F}^w as

$$\begin{aligned} \mathbf{V}_{\mathbb{F}}(f_1, \dots, f_v) &= \mathbf{V}(f_1, \dots, f_v) \cap \mathbb{F}^w \\ &= \{\mathbf{x} \in \mathbb{F}^w \mid f_1(\mathbf{x}) = \dots = f_v(\mathbf{x}) = 0\} \end{aligned}$$

We say that a $v \times w$ matrix is strongly-regular if all its $r \times r$ minors are regular for all $1 \leq r \leq v$. For instance, if \mathbb{F} is a field with at least w distinct nonzero elements $\gamma_1, \dots, \gamma_w$, then $A_{i,j} = \gamma_j^i$ is strongly-regular.

Lemma 10: (Theorem 3.2 [7]) Let $v \geq 1, \varepsilon > 0$ and \mathbb{F} be a finite field. Let $w = v/\varepsilon$ and w divides n . Let A be a $v \times w$ matrix with coefficients in \mathbb{F} which is strongly-regular. Let $d_1 > \dots > d_w$ be integers. For $i \in [v]$ let

$$f_i(x_1, \dots, x_w) = \sum_{j=1}^w A_{i,j} x_j^{d_j}$$

and define the subspace evasive sets $\mathcal{S} \in \mathbb{F}^n$ to be (n/w) times cartesian product of $\mathbf{V}_{\mathbb{F}}(f_1, \dots, f_v) \subset \mathbb{F}^w$. That is

$$\begin{aligned} \mathcal{S} &= \mathbf{V}_{\mathbb{F}}(f_1, \dots, f_v) \times \dots \times \mathbf{V}_{\mathbb{F}}(f_1, \dots, f_v) \\ &= \{\mathbf{x} \in \mathbb{F}^n : f_i(x_{tw+1}, \dots, x_{tw+w}) = 0, \\ &\quad \forall 0 \leq t < n/w, 1 \leq i \leq v\} \end{aligned}$$

Then \mathcal{S} is $(v, (d_1)^v)$ -subspace evasive sets.

Moreover, if at least v of the degrees d_1, \dots, d_w are co-prime to $|\mathbb{F}| - 1$, then $|\mathcal{S}| = |\mathbb{F}|^{(1-\varepsilon)n}$.

The size of list is bounded by d_1 and v . If we can bound d_1 by v , the list size can be only bounded by the v -dimension subspace \mathcal{H} .

Lemma 11: (Claim 4.3 [7]) There exists a constant $C > 0$ such that the following holds: There is a deterministic algorithm that, given integer inputs v, N so that in $\text{Poly}(N)$ time there is prime q and v integers $v^{C \log \log v} > d_1 > d_2 > \dots > d_v > 1$ such that:

- 1) For all $i \in [v]$, $\gcd(q-1, d_i) = 1$
- 2) $N < q \leq N \cdot v^{C \log \log v}$

Because we only need to choose w integer $d_1 > \dots > d_w$ and v of the integers are co-prime to q , the bound of $d_1 \leq \max(w, v^{C \log \log v})$.

B. Encoding Vector as Elements in \mathcal{S}

We show the encoding map $\text{SE} : \mathbf{v} \rightarrow \mathbf{s}$. Assuming there is a vector \mathbf{v} of length n_1 and $(w-v)|n_1$. First we divide the vector into $\frac{n_1}{w-v}$ blocks. Then for each block \mathbf{v}_i for $i = 1, \dots, \frac{n_1}{w-v}$, we encode into a block \mathbf{s}_i using bijection φ . Then we concatenate each block \mathbf{s}_i for $i = 1, \dots, \frac{n_1}{w-v}$ and generate \mathbf{s} in \mathcal{S} . We give the function φ in the following.

Lemma 12: (Claim 4.1) Assume that at least v of the degree d_1, \dots, d_v are co-prime to $|\mathbb{F}| - 1$. Then there is an easy to compute bijection $\varphi : \mathbb{F}^{w-v} \rightarrow \mathbf{V}_{\mathbb{F}} \subset \mathbb{F}^w$. Moreover, there are $w-v$ coordinates in the output of φ that can be obtained from the identity mapping $\text{Id} : \mathbb{F}^{w-v} \rightarrow \mathbb{F}^{w-v}$.

Let d_{j_1}, \dots, d_{j_v} be the degree among d_1, \dots, d_w co-prime to $|\mathbb{F}| - 1$ and let $J = \{j_1, \dots, j_v\}$ and $x_{j_i}^{d_{j_i}} = y_i$. On the positions $[w] \setminus J$, the map φ takes the elements from \mathbb{F}^{w-v} to $\mathbb{F}^{[w] \setminus J}$. For the elements on J , there is

$$\sum_{j \in J} A_{i,j} x_j^{d_j} = - \sum_{j \notin J} A_{i,j} x_j^{d_j}$$

Let A' be the $v \times v$ minor of A given by restricting A to columns in J and $b_i = - \sum_{j \notin J} A_{i,j} x_j^{d_j}$. Then

$$A' y = b$$

and for each y , there is unique solution of $x_{j_i}^{d_{j_i}} = y_i \pmod{q}$ because d_{j_i} is co-prime to $q-1$.

C. Computing Intesection

We show how to compute the intersection $\mathcal{S} \cap \mathcal{H}$ given (v, ℓ_{SE}) subspace evasive sets \mathcal{S} and v -dimension subspace \mathcal{H} . The subspace evasive sets \mathcal{S} will filter out the elements in \mathcal{H} and output a set of elements $\mathcal{S} \cap \mathcal{H}$ with size no more than ℓ_{SE} .

Lemma 13: (Claim 4.2 [7]) Let $\mathcal{S} \subset \mathbb{F}^n$ be the (v, ℓ_{SE}) -subspace evasive sets. There exists an algorithm that, given a basis of \mathcal{H} , output $\mathcal{S} \cap \mathcal{H}$ in $\text{Poly}((d_1)^v)$ time.

Because \mathcal{H} is v -dimensional subspace and $\mathcal{H} \subset \mathbb{F}^n$, there exists a set of affine maps $\{\ell_1, \dots, \ell_n\}$ such that for any elements $\mathbf{x} = \{x_1, \dots, x_m\} \in \mathcal{H}$, there is $x_i = \ell_i(s_1, \dots, s_v)$.

We show the result by induction of the number of blocks $i = 1, \dots, n/w$. If $i = 1$, let $\mathcal{H}_1 := \{(x_1, \dots, x_w) : (x_1, \dots, x_n) \in \mathcal{H}\}$, the dimension of \mathcal{H}_1 is $r_1 \leq v$ and $\mathcal{H}_{x_1, \dots, x_w} = \{(x_1, \dots, x_n) \in \mathcal{H} : (x_1, \dots, x_w) \in \mathcal{H}_1\}$ such that $\mathcal{H} = \cup_{(x_1, \dots, x_w) \in \mathcal{H}_1} \mathcal{H}_{x_1, \dots, x_w}$, and the dimension of $\mathcal{H}_{x_1, \dots, x_w}$ is $v - r_1$. There is

$$\begin{aligned} &\mathbf{V}_{\mathbb{F}}(f_1, \dots, f_v) \cap \mathcal{H}_1 \\ &= \{(x_1, \dots, x_w) = (\ell_1(s_1, \dots, s_v), \dots, \ell_w(s_1, \dots, s_v)) : \\ &\quad f_1(\ell_1(s_1, \dots, s_v), \dots, \ell_w(s_1, \dots, s_v)) = 0, \dots, \\ &\quad f_v(\ell_1(s_1, \dots, s_v), \dots, \ell_w(s_1, \dots, s_v)) = 0\} \end{aligned}$$

We can solve the v equations to get (s_1, \dots, s_v) and then obtain (x_1, \dots, x_w) . Since $\mathcal{H}_1 \subset \mathbb{F}^w$,

$$\mathbf{V}_{\mathbb{F}}(f_1, \dots, f_v) \cap \mathcal{H}_1 = \mathbf{V}(f_1, \dots, f_v) \cap \mathcal{H}_1$$

By Bezout's theorem, there is $|\mathbf{V}(f_1, \dots, f_v) \cap \mathcal{H}_1| \leq (d_1)^{r_1}$. So there are at most $(d_1)^{r_1}$ solutions for $(x_1, \dots, x_w) \in \mathcal{H}_1$. The computational time of solving the equation system follows from powerful algorithms that can solve a system of polynomial equations (over finite fields) in time polynomial in the size of the output, provided that the number of solutions is finite in the algebraic closure (i.e the zero-dimensional case). So for $i = 1$, the computational time is at most $\text{Poly}((d_1)^{r_1})$ and there are $(d_1)^{r_1}$ solutions for (x_1, \dots, x_w) .

For every fixed of the first w coordinates, we reduce the dimension of \mathcal{H} by r_1 and obtained a new subspace \mathcal{H}_2 on the remaining coordinates. Continuing in the same fashion with \mathcal{H}_2 on the second block we can compute all the solutions in times $\text{Poly}((d_1)^{r_1}) \cdot \text{Poly}((d_1)^{r_2}) \cdots \text{Poly}((d_1)^{r_{n/w}})$, where $r_1 + r_2 + \dots + r_{n/w} = v$. So the total running time is $\text{Poly}((d_1)^v)$.

APPENDIX B LIST DECODABLE CODE

A. Decoding algorithm of FRS code

Linear algebraic list decoding [8] has two main steps: interpolation and message finding as outlined below.

- Find a polynomial, $Q(X, Y_1, \dots, Y_v) = A_0(X) + A_1(X)Y_1 + \dots + A_v(X)Y_v$, over \mathbb{F}_q such that $\deg(A_i(X)) \leq D$, for $i = 1 \dots v$, and $\deg(A_0(X)) \leq D + k - 1$, satisfying $Q(\alpha_i, y_{i1}, y_{i2}, \dots, y_{iv}) = 0$ for $1 \leq i \leq n_0$, where $n_0 = (u - v + 1)N$.
- Find all polynomials $f(X) \in \mathbb{F}_q[X]$ of degree at most $k - 1$, with coefficients $f_0, f_1 \dots f_{k-1}$, that satisfy, $A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \dots + A_v(X)f(\gamma^{v-1}X) = 0$, by solving linear equation system.

The two above requirements are satisfied if $f \in \mathbb{F}_q[X]$ is a polynomial of degree at most $k - 1$ whose FRS encoding agrees with the received word \mathbf{y} in at least t components:

$$t > N\left(\frac{1}{v+1} + \frac{v}{v+1} \frac{uR}{u-v+1}\right)$$

This means we need to find all polynomials $f(X) \in \mathbb{F}_q[X]$ of degree at most $k - 1$, with coefficients f_0, f_1, \dots, f_{k-1} , that satisfy,

$$A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \dots + A_v(X)f(\gamma^{v-1}X) = 0$$

Let us denote $A_i(X) = \sum_{j=0}^{D+k-1} a_{i,j}X^j$ for $0 \leq i \leq v$. ($a_{i,j} = 0$ when $i \geq 1$ and $j \geq D$). Define the polynomials,

$$\begin{cases} B_0(X) = a_{1,0} + a_{2,0}X + a_{3,0}X^2 + \dots + a_{v,0}X^{v-1} \\ \vdots \\ B_{k-1}(X) = a_{1,k-1} + a_{2,k-1}X + a_{3,k-1}X^2 + \dots \\ + a_{v,k-1}X^{v-1} \end{cases}$$

We examine the condition that the coefficients of X^i of the polynomial $Q(X) = A_0(X) + A_1(X)f(X) + A_2(X)f(\gamma X) + \dots + A_v(X)f(\gamma^{v-1}X) = 0$ equals 0, for $i = 0 \dots k - 1$. This is equivalent to the following system of linear equations for $f_0 \dots f_{k-1}$.

$$\begin{bmatrix} B_0(\gamma^0) & 0 & 0 & \dots & 0 \\ B_1(\gamma^0) & B_0(\gamma^1) & 0 & \dots & 0 \\ B_2(\gamma^0) & B_1(\gamma^1) & B_0(\gamma^2) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ B_{k-1}(\gamma^0) & B_{k-2}(\gamma^1) & B_{k-3}(\gamma^2) & \dots & B_0(\gamma^{k-1}) \end{bmatrix} \times \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{k-1} \end{bmatrix} = \begin{bmatrix} -a_{0,0} \\ -a_{0,1} \\ -a_{0,2} \\ \vdots \\ -a_{0,k-1} \end{bmatrix} \quad (8)$$

The rank of the matrix of (Eqs. 8) is at least $k - v + 1$ because there are at most $v - 1$ solutions of equation $B_0(X) = 0$ so at most $v - 1$ of γ^i that makes $B_0(\gamma^i) = 0$. The dimension of solution space is at most $v - 1$ because the rank of matrix of (Eqs. 8) is at least $k - v + 1$. So there are at most q^{v-1} solutions to (Eqs. 8) and this determines the size of the list which is equal to q^{v-1} .

APPENDIX C PROOF OF LEMMA 8

Proof: FRS decoding algorithm FRSdec requires,

$$N - \rho_w N > N\left(\frac{1}{v+1} + \frac{v}{v+1} \frac{uR_{\text{FRS}}}{u-v+1}\right) \quad (9)$$

The dimension of the FRS code is bounded by,

$$\begin{aligned} k &= uR_{\text{FRS}}N = w \lceil \frac{\ell N + 2N}{w-v} \rceil + u\rho_r N \\ &\leq \frac{w}{w-v} (uRN + 3N) + u\rho_r N. \end{aligned} \quad (10)$$

The (10) holds because $\ell \leq uR + 1$. So the decoding condition for FRS code (9) holds if,

$$N - \rho_w N > N\left(\frac{1}{v+1} + \frac{v}{v+1} \frac{\frac{w}{w-v}(uR+3) + u\rho_r}{u-v+1}\right)$$

From $w = v^2$, it is equivalent to,

$$\rho_w < \frac{v}{v+1} - \frac{v}{v+1} \frac{\frac{v}{v-1}(uR+3) + u\rho_r}{u-v+1}.$$

■